UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/804,591	03/19/2004	Trevor William Freeman	13768.497	9557

47973 7590 05/07/2007

WORKMAN NYDEGGER/MICROSOFT
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UT 84111

EXAMINER	
MEDE, ESTEVE	

ART UNIT	PAPER NUMBER
2109	

MAIL DATE	DELIVERY MODE
05/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/804,591	FREEMAN ET AL.	
	Examiner	Art Unit	
	Esteve Mede	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *04/06/2006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Claim Objections

1. **Claims 1, 3-4, 6, 8-9, 15, 17 and 24,** are objected to because of the following informalities: in claim 1, line 2 the term "used to can authenticate with a server" should be --used to authenticate with a server--; in claim 1, line 9 the term of " the additional credentials" should be --the additional credential--; in claim 3, line 1 the term "establishing a secure link" should be --establishing the secure link--; in claim 4, line 1 the term the an act of receiving and additional credential" should be --the act of receiving the additional credential--; in claim 6, line 1 the term "establishing a secure link" should be –establishing the secure link--; in claim 8, line 1-2, the term "provisioning an additional credential" should be--provisioning the additional credential--; in claims 9 and 19, line 8 the term "the client computing system and server" should be --the client computing system and the server--; in claim 15, line 1-2 the term "a second server request" should be --the second server request--; in claim 17, line 1-2 the term "sending a second response" should be --sending the second response--; in claim 24, line 1-2 the term "identifying a tunnel key" and "deriving a tunnel key" should be --identifying the tunnel key --and deriving the tunnel key--; . Appropriate correction is required.

Claims 2-4 and 9-18 and 22 are also objected to as they are depending upon claims 1 and 9.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. **Claims 1-9, 11-12 and 19** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jerdoneck (US 6,983,381 B2).

Claims 1-8, Jerdoneck discloses In a client computing system, a method for receiving credentials that can be used to can authentic with a server computing system, the method comprising: an act of receiving a limited-use credential (i.e. one-time password) (col. 6, lines 66-67); an act of establishing a secure link between the client computing system and the server computing system (the prior art discloses a secure connection between the client and the server and server to client, therefore the limitation of a secure link between the server and the client is met (col. 6, lines 34-63)); an act of submitting the limited-use credential to the server computing system over the established secure link (the prior art discloses a secure connection between the client and the server and server to client, therefore the limitation of a secure link between the server and the client is met (col. 7, lines 1-12; lines 15-38)); and an act of receiving an additional credential that can be used for subsequent authentication with the server computing system (the prior art discloses a certificate along with the one-time password for subsequent authentication (col. 5, lines 53-56; col. 8, lines 60-65; col. 3, lines 50-53)); however Jerdoneck does not disclose that the additional credentials being

provisioned at the sever computing system based on the limited-use credential. The general concept of provisioning a certificate at the server computing system is a well known process within the art, and therefore no additional explanation will be provided; limitation of a session key is implicitly stated by the prior as the messages are encrypted between the client and the server and are using a secure link for communication). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Jerdoneck in order to provide secure communication between two or more parties.

Claims 9 and 19, Jerdoneck discloses, In a client computing system, a method for participating in authentication with a server computing system, the method comprising: an act of receiving a first server request that includes at least the authentication mechanisms deployed at the server computing system (the prior art discloses an authentication mechanism deployed at the server side (see col. 6, lines 55-63)); an act of sending a first response that includes at least the authentication mechanisms deployed at the client computing system (col. 6, lines 66-67; col. 7, lines 1-5); an act of identifying a tunnel key that can be used to encrypt content transferred between the client computing system and server computing system (the prior art disclose a secure transaction between the client and the server and between the server and the client using strong encryption to encrypt contents, which are being transferred among the parties (col. 7, lines 6-12); however Jerdoneck does not disclose an act of receiving a second server request that includes encrypted

authentication content, the encrypted authentication content being encrypted with the tunnel key; an act of decrypting the encrypted authentication content with the tunnel key to reveal unencrypted authentication content, the unencrypted authentication content indicating a mutually deployed authentication mechanism; and an act of sending a second response, the second response including encrypted response data that is responsive to the unencrypted authentication content, the encrypted response data for authenticating with the server computing system according to the mutually deployed authentication mechanism. The general concept of encrypting the authentication content with a tunnel key; decrypting the content with the tunnel key to reveal the content unencrypted and sending a response an encrypted response base upon the unencrypted authentication, thus that the client may communicate with the server is an implicit property of the prior art, as it would be impossible for the server and client to communicate securely without agreed upon cryptographic keys, for example the server would not be able to decrypt the content of the client and the client would not be able to decrypt the contents of the server, therefore authentication among the server and the client would not take place as they would not be able to understand each other encryption key bits. Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Jerdoneck in order to provide secure communication between two or more parties.

Claims 11-12 and 21-22, Jerdoneck discloses the method wherein the authentication mechanism deployed at the server computing system include one more authentication mechanism a token for authentication (the prior art discloses the use of

a Token and Certificate for authentication (see, col. 7, lines 20-25)) a certificate from a Certificate Authority (x.509) for authentication (col. 7, lines 9-10) and a hash (MD5, Sha-1).

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 10, 13, 16, 18, 20, and 23-28** are rejected under 35 U.S.C. 103(a) as being unpatentable over Jerdoneck (US 6,983,381 B2) in view of Salgarelli et al. (EAP-Shared Key Exchange (EAP-SKE): A Scheme for Authentication and Dynamic Key Exchange in 802.1X Networks, April 30, 2002).

Claims 10, 13, 16, 18, 20, 23, 26 and 28, Jerdoneck discloses the method wherein the first response in includes the authentication mechanisms deployed at the client include one or more public keys (see abstract) however Jerdoneck does not disclose that the authentication mechanisms deployed at the server computing system, a previous packet ID and a Nonce. The general concept of the first server request includes the authentication mechanisms deployed at the server computing system, a previous packet ID and a Nonce is well known in the art as illustrated by Salgarelli,

which discloses the request includes the authentication deployed at the server computing system a previous packet ID and a Nonce (see page 8, section 3.3 Protocol description, see also Figure 2). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Jerdoneck to include the use of Salgarelli in order to prevent replay attack.

Claims 14, and 24, Jerdoneck discloses all the limitation of claim 14 except for The method as recited in claim 9, wherein the act of identifying a tunnel key comprises deriving a tunnel key based on a shared secret, a client side nonce, and a server side nonce. The general concept of identifying a tunnel key based on a shared secret is well known in that art as illustrated by Salgarelli, which discloses a shared secret key and Nonces (see abstract on page 2; see page 8, section 3.3 Protocol description, see also Figure 2). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Jerdoneck to include the use of Salgarelli in order to share information securely in a wireless network or VPN.

Claims 15, 17, 25 and 27, Jerdoneck discloses all the limitation of claim 15, except for the method as recited in claim 9, wherein the act of receiving a second server request comprises receiving encrypted authentication content corresponding to an authentication method selected from among: negotiating an authentication method, re-authenticating, boot-strapping a client with an existing user-name and password, boot-strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token. The general concept of receiving encrypted authentication content corresponding to an authentication

method selected from among: negotiating an authentication method, re-authenticating, boot-strapping a client with an existing user-name and password, boot-strapping a client with an X.509 certificate, authenticating with an X.509 certificate, and boot-strapping a new client with a Kerberos token is well known within the art as illustrated by Salgarelli, which discloses re-authentication, secure token (see Section 9 "Open Issues on page 17-18). Therefore it would have been obvious for one of ordinary skill in the art at the time of the invention to modify Jerdoneck to include the use of Salgarelli in order to provide secure communication between the server and client.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Esteve Mede whose telephone number is 571-270-1594. The examiner can normally be reached on Monday thru Friday, 8:30-5:00 PM, EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Frantz Jules can be reached on 571-272-6681. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Esteve Mede
em
April 19, 2007

FRANTZ JULES
SUPERVISORY PATENT EXAMINER